Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 3, 10, 11, and 13-31 are pending in the application, with claims 11, 25, and 30 being the independent claims. Claims 1 and 9 are sought to be cancelled without prejudice to or disclaimer of the subject matter therein. Claims 3, 10, 11, 13, and 23-27 are sought to be amended. New claims 30 and 31 are sought to be added. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 112

In the Office Action, independent claim 11 and new dependent claims 23, 24, 26, and 27 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirements. Claims 13-22, 28, and 29 were rejected based on their dependency. Applicants respectfully traverse this rejection.

Specifically, the Office Action states that the "specification/original disclosure fails to mention/specify or teach the following limitation ... "**generate a pseudo-random number as a result of a second RC4 shuffling operation**; byte-wise transfer a portion of the data to the combinational logic block **as a first input value, transfer the generated pseudo-random number to the combinational logic as a second input value.**" (Office Action, p. 6)(emphasis in the original).

The specification provides adequate written description support for these limitations. The specification describes a key setup process during which the state machine directs a shuffling operation that includes swapping the i^{th} and j^{th} elements of the state memory in step 606. (Specification, p. 10, lines 23-24). Step 606 describes a portion of a first "RC4 shuffling operation." The specification further describes the ciphering operation performed during an RC4 stream cipher. (Specification, p. 11, lines 1-12). As part of the ciphering operation, at step 708, the i^{th} and j^{th} elements of the state memory are swapped. (Specification, p. 11, lines 6-7). This step describes a portion of the second "RC4 shuffling operation." The nth element of the state memory (identified as a result of step 709) is the random value generated as a result of an RC4 random byte generation process represented by steps 704-709 of FIG. 7 (and described in Schneier). Schneier explains that the output of the RC4 random byte generation process is a "random byte." (Schneier, p. 397). Thus, Applicants' specification provides adequate written description support for the limitation "generate a random byte as a result of a second RC4 shuffling operation."

The specification further describes that an output byte is formed by combining the nth element of the state memory (random byte/second input value) with the data byte to be encrypted (portion of the data/first input value) using a bit by bit exclusive OR operation (combinational logic). Thus, Applicants' specification provides adequate written description support for the limitation "byte-wise transfer a portion of the data to the combinational logic block as a first input value, transfer the generated random byte to the combinational logic as a second input value."

These citations, among others, show that the specification describes the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. See, e.g., *Moba, B.V. v. Diamond Automation, Inc.*, 325 F.3d 1306, 1319, (Fed. Cir. 2003). Reconsideration and withdrawal of this rejection is therefore respectfully requested.

Rejections under 35 U.S.C. § 103

In the Office Action, claims 1, 3, 9-11, and 13-29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Johns-Vano, et al, EP Patent Publication No. EP0895164 (Vano) in view of Schneier, "Applied Cryptography," Chapter 17 "Other Stream Ciphers and Real Random-Sequence Generation." (Schneier). Applicants respectfully traverse this rejection.

The combination of Vano and Schneier does not teach or suggest each and every limitation of amended independent claims 11 and 25 or new independent claim 30. Vano generally describes a cryptographic co-processor (CCO 550) which is "preferably configured to perform combiner type cryptographic operations." (Vano, col. 5, lines 40-41). Vano does not teach or suggest cryptographic operations required by an RC4 stream cipher and thus, does not describe that these operations are directed by a state machine and performed completely within a cryptographic accelerator. As described in Applicants' specification, an RC4 stream cipher includes RC4 shuffling operations which require a sequence of swapping operations to move substitution values between memory locations. (Specification, p. 10, lines 17-29; p. 11, lines 1-12).

Nowhere does Vano teach or suggest a state machine "configured to direct an RC4 shuffling operation by which the plurality of substitution values are moved to different memory locations within the state memory, wherein the shuffling operation is completely performed within the cryptographic accelerator" as recited in new independent claim 30.

Furthermore, nowhere does Vano teach or suggest:

> a state machine coupled to the combinational logic block and the state memory, the state machine configured to:
>
> initialize via hardware an incrementing pattern of substitution values in the state memory, each substitution value stored in as separate memory location
>
> perform a first RC4 shuffling operation using a portion of a key array received from a system memory, wherein the first RC4 shuffling operation is performed concurrently with the receipt of the portion of the key array,
>
> generate a random byte as a result of a second RC4 shuffling operation;
>
> byte-wise transfer a portion of the data to the combinational logic block as a first input value,
>
> transfer the generated random byte to the combinational logic as a second input value,
>
> logically operate on the first and second input values by the combinational logic to form a resulting data byte, and outputting the resulting data byte.

as recited in amended independent claim 11. Furthermore, Vano does not teach or suggest a method including "(c) upon direction of a state machine, shuffling the pattern of substitution values in the state memory using an RC4 shuffling operation, wherein the shuffling is performed concurrently with the receipt of the portion of the key array, and wherein the shuffling operation is completely performed within the cryptographic accelerator; and (d) repeating steps (b) and (c) until each portion of the key array has been received," as recited in amended independent claim 25.

Schneier does not overcome these deficiencies of Vano. Schneier generally describes the RC4 stream cipher. Schneier does not teach or suggest any techniques for implementing or accelerating the RC4 stream cipher. Accordingly, the combination of Vano and Schneier does not teach or suggest each and every limitation of independent claims 11, 25, and 30.

For at least these reasons, independent claims 11, 25, and 30 are patentable over the combination of Vano and Schneier. Claims 3, 10, 22, 24, and 31 depend from claim 30; claims 13-22 depend from claim 11; and claims 26-29 depend from claim 25. For at least the above reasons, and further in view of their own features, claims 3, 10, 13-22, 24, 26-29, and 31 are patentable over the combination of Vano and Schneier. Reconsideration and withdrawal of this rejection is therefore respectfully requested.

Claim Objections

In the Office Action, claim 13 was objected to because claim 13 "is dependent on the canceled claim 12." As suggested by the Examiner, claim 13 was amended to depend from claim 11. Reconsideration and withdrawal of this objection is therefore respectfully requested.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for

allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Applicant
Registration No. 50,633

Date: 2-7-07

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

585491_1.DOC